

What's Keeping IoT Executives Up At Night in 2019

A Study from Internet of Things World

Introduction

The promise of IoT is enormous, from reducing operating costs, to improving workplace safety; yet many organizations face hurdles when it comes to implementation. The top three concerns for IoT leaders in 2019 are execution, cybersecurity, and initial purchase cost. These are the conclusions from a survey by the organizers of [IoT World 2019](#), the largest IoT conference in the world taking place May 13-16 in Santa Clara, California, which surveyed more than 100 IoT leaders across a range of industries. Survey respondents included IoT leaders in manufacturing, telecoms, healthcare, retail, construction, supply chain and logistics, oil and gas/energy, government, transportation and agriculture.

Implementation & Security Are Top Challenges

Implementation and security are the clear top concerns for IoT leaders across industries, with initial purchase cost rounding out the top three. Most decision makers are not concerned about ongoing upkeep costs, likely anticipating or already seeing ROI based on improved efficiencies. The full list of concerns ranks as follows:

1. Implementing the technology (34%)
2. Security (25%)
3. Initial purchase (17%)
4. Scalability (10%)
5. Business buy-in (8%)
6. Upkeep costs (3%)

Among those surveyed, 66% say their C-Suite executives are supportive of their IoT implementation plans, but that support does not solve the challenges around effectively implementing the technology or ensuring ecosystem security. These top two concerns – implementation and security – go hand in hand. Before any enterprise can implement new IoT technology, companies must do their due diligence on potential security risks, their staff's readiness to support the new technology and how to properly deploy it.

At the front end of this challenge, 45% of companies say they are deploying IoT devices on a dedicated network to mitigate security risk. Additionally, 46% are introducing internal training systems for their entire workforce, which will improve the efficacy of the devices and limit vulnerability due to an oversight. Once the devices are successfully deployed decision makers are focused on maintaining security by doing all of the 'small things' right:

- 68% are regularly updating firmware and software
- 44% are checking devices to see if physical access to the devices makes them vulnerable to hacking
- 35% are making data decryption a default

Internet of Things World

- 26% are shutting down devices when they are not in use
- 17% are leveraging Blockchain to enhance security

“Cyber threats come from so many different directions for the modern enterprise. So often the difference between being compromised and being secure is having done the checklist of best practices, like making sure every device has the latest software updates. Our research showed that luckily IoT executives are very aware of this reality.”

– Zach Butler, Director, IoT World

Preparing for Additional IoT Implementation: Hiring & Training

With additional IoT implementation expected, IoT leaders are focusing on training and hiring to support this growing ecosystem. In addition to 46% of companies focusing on internal training for their entire workforce, companies are also building out their roster of specialist:

- 64% plan on training current employees for new, more technical, roles
- 63% plan on hiring new employees
 - 33% additional data analysts
 - 30% a different technical role
- 10% plan to hire more remote employees

Blockchain & 5G Networks

While organizations are building out their expertise and constantly exploring new technology, they are also being judicious in which technologies they are implementing. Although blockchain was a heavily discussed topic in 2018, IoT leaders were evenly split on how effective blockchain was as a tool to improving their ecosystem security. When asked the primary benefit of combining blockchain with IoT, respondents answered:

- IoT architectures that rely on centralized servers to collect and store data will be able to write local ledgers that will sync with other localized ledgers to maintain a single, yet secure copy of the truth. (15%)
- Blockchain due to its background in high-end cryptography helps with IoT security. (29%)
- Smart contracts can be applied to the data in the blockchain to enforce business conditions on the IoT interactions. (13%)
- IoT transactions on the Blockchain will be timestamped, ensuring that they are available when needed. (12%)

- I don't see a benefit (29%)

Although widespread 5G rollouts are not expected until 2020, many companies would be interested in leveraging it this year if they had the option:

- 41% saying they would deploy IoT devices on a 5G network this year if it is available
- 37% would take a wait and see approach on 5G and instead stick with their current wireless network
- 22% do not rely on wireless networks for their IoT deployment

“5G will be a key enabler for smart cities, autonomous vehicles and industrial IoT. It will offer important capabilities for IoT applications needing high bandwidth, very low latency, and ultra-reliability, and - once coverage and devices become more widely available - for massive-scale IoT deployments. But in the meantime enterprises looking to deploy IoT have a wide variety of other technology options to choose from; the diversity of IoT requirements means no single solution will dominate.”

– Alexandra Rehak, Internet of Things Practice Head, Ovum

For additional information on the issues the IoT industry is facing, check out the panels at [IoT World 2019](#) where our speakers will be addressing these topics, with focus areas including Industrial IoT, Smart Home, Smart Cities, Security, Edge Computing, Smart Buildings and Construction, AI, Healthcare, Energy and Utilities, Transportation and more.